

**U.S. Department of Commerce  
National Institute of Standards and Technology  
(NIST)**



**Privacy Threshold Analysis  
for the  
150-01 Office of Safety, Health, and Environment**

## **U.S. Department of Commerce Privacy Threshold Analysis**

### **National Institute of Standards and Technology (NIST)**

**Unique Project Identifier: 150-01**

**Introduction:** This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based on Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

**Description of the information system and its purpose:** *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- a) Whether it is a general support system, major application, or other type of system*
- b) System location*
- c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
- d) The purpose that the system is designed to serve*
- e) The way the system operates to achieve the purpose*
- f) A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) Identify individuals who have access to information on the system*
- h) How information in the system is retrieved by the user*
- i) How information is transmitted to and from the system*

**The Office of Safety, Health, and Environment (OSHE) supports NIST in carrying out its mission safely and in maintaining safety as an integral core value and vital part of the NIST culture. The OSHE information system supports this role and includes the following components:**

- **The Radiation Monitoring System (RMS) is used to monitor radioactive sources above a certain level. The RMS has detectors, processors, cameras, and network connectors monitoring sensitive equipment and their surrounding physical locations. The monitoring provides unidirectional information to NIST Emergency Services consoles. This component does not contain PII records that are retrievable by a unique identifier.**

- **The Health Physics System (a.k.a., HAPPY) provides inventory of radioactive material, ionizing machines, radiation equipment, physical radiation laboratories. HAPPY has also been used since 2007 to track NIST staff radiation exposure. In addition, required safety training is made available through the internal, web-based Safety Education and Training (SET) site to ensure training prior to access to radioactive material, machines, equipment, or laboratories. SET is an OSHA application used to provide and track training.**
- **The Health Unit (HU) provides health services to federal employees/contractors, member of the public, foreign nationals, or visitors who require care related to their position or while on Gaithersburg's campus. The HU is not a Covered Entity under HIPAA. Both Occupational Health Records and Personal Health Records are maintained in case files. Case files dated 2018 and prior are maintained as paper records, whereas case files dated 2019 to present are maintained in the Health Unit's Electronic Medical Records System (EMRS).**
- **The EMRS is a COTS cloud-based application used to enable online scheduling of appointments, tracking patient visits, storing health data, such as audiometer and spirometer test results, vaccination and test results, photographs of wounds or injuries, prescriptions, etc., and includes information related to maintenance of a Commercial Driver's License. All staff may log into EMRS to access their own record, although only medical information collected during medical appointments made since 2019 is available in the system. Visits prior to 2019 are only on paper records, which patients can request to see.**
- **The Tort process and some safety incident investigations require collection of PII or PHI for claims for damage, injury, death, or motor vehicle accident reports. This process could include police reports if applicable. OSHA assists in the investigation and reporting processes but does not maintain any documents. Legal documents are sent to Human Resources, DOC, and/or physical security.**

*a. Whether it is a general support system, major application, or other type of system*

**150-01 is a General Support System.**

*b. System location*

**The EMRS is a COTS cloud-based application hosted within the continental United States. All other system components are located at the NIST Gaithersburg, Maryland and Boulder, Colorado facilities within the continental United States.**

*c. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

**The RMS is a standalone component and only communicates with devices located in the Emergency Services guard offices via a private network in Buildings 101 and 318 over OSHA's isolated Research Equipment Network (REN).**

**The HAPPY is a standalone database.**

The EMRS is a standalone application housed in an encapsulated environment but obtains a weekly report from the Central People Repository (NIST 183-01) with NIST employee and associate data. This file is transferred to the EMRS via Secure FTP for purposes of account generation, allowing Single Sign On (SSO) to the ERMS with employment status, supervisor or host information, and contact information for staff.

All system connectivity to HAPPY and the Health Unit is via TCP/IP across the NIST Network Infrastructure (NIST 181-04) to encrypted file share (NIST 184-12). NIST 181-04 provides all services for physical cabling, network frame synchronization/flow control/error checking, routing, switching, and DNS. All data is encrypted with FIPS 140-2 compliant technologies in transit and at rest.

*d. The purpose that the system is designed to serve*

The 150-01 system contains the hardware and software required by the NIST Office of Safety, Health, and Environment (OSHE) staff to provide support to help reduce safety, health, and environmental (SH&E) risks at NIST by planning, developing and maintaining, supporting the implementation of, overseeing compliance with, and continually improving NIST's SH&E programs. In doing so, OSHE enables NIST to carry out its mission effectively and efficiently while protecting the worker, the public, and the environment and complying with applicable laws and regulations. Additionally, the 150-01 system includes safety-related applications that are available to and used by all NIST staff in support of the OSHE and NIST mission.

*e. The way the system operates to achieve the purpose*

The RMS provides monitoring capabilities via a live video feed for Emergency Services to detect unauthorized access to radioactive material.

The HAPPY provides access and inventory of radioactive materials and related information, which are stored and tracked in the HAPPY database application. Owners of radioactive material access and update the database via secured, authorized computers.

The Health Unit (HU) component provides scheduling of appointments, tracking patient visits, storing health data, such as audiometer and spirometer test results, vaccination and test results, photographs of wounds or injuries, prescriptions, etc. The HU component includes maintaining legacy medical case files in paper form, and an Electronic Medical Record System (EMRS). With the implementation of EMRS, while all active NIST staff have access to ERMS, not all medical records were transitioned (i.e., scanned and uploaded).

- For patients who received care from 2019 to present, Health Unit medical case files includes scans of all paper records generated during patient visit.
- For patients who have not received care since 2019 (e.g., calendar year 2018 and prior), medical case files remain as a paper record until the next time health services are rendered. At that time, some of the medical information may be

transitioned to EMRS, while the majority will continue to remain in the paper medical case file.

Access to medical case files, whether legacy paper files or within the EMRS, is restricted using role-based access controls. For example, the EMRS has role-based access controls restricting access and views for health practitioners, health unit administrative staff, and system administrators. Patients can log into EMRS to view their personal information and appointments. Supervisors can only see their employee and associates occupational health appointments to determine if required tests are scheduled. The legacy paper case files continue to be stored in a secured location and cabinets until they are needed by the patient or administrative staff, or it is time to archive or destroy. The National Archives and Records Administration (NARA) does not currently have the capability to receive electronic records for archival, so Occupational Health records are printed (as necessary) and archived with NARA according to the Records Schedule.

Tort claims are initiated with the forms:

- **SF-95 Claim for Damage, Injury or Death** – to be used by a non-federal person making such claims against NIST pursuant to the Federal Tort Claims Act.
- **SF-91 Motor Vehicle Accident Report** – Used by operators of federal motor vehicles for every motor vehicle accident involving injury, fatality, and/or damage exceeding \$500.
- **GSA Form 1627 Motor Vehicle Accident Reporting Kit** – to assist vehicle operators involved in an incident with a GSA leased fleet vehicle.

*f. A general description of the type of information collected, maintained, used, or disseminated by the system*

**RMS provides a live camera feed for emergency service employees to monitor and prevent physical access to radiation areas. The RMS has detectors, processors, cameras, and network connectors. There are no input/output devices on the systems; they feed and are controlled by systems located in the physical security guard's office in Buildings 101 and 318. They are on a dedicated private network, cannot communicate with each other and only to the Emergency Service Division's consoles. The RMS systems records all camera activity to a DVR in the Emergency Services Division (ESD) space. DVR will recycle and overwrite previous activity unless an alarm is activated at which time the system will prevent data from being overwritten.**

**HAPPY collects inventory and dosimetry results of radioactive material via the owner's input into the database. This includes any exposures. The SSNs of material owners are required for reporting purposes to the Nuclear Regulatory Commission to retain our license to work with radioactive material.**

**Health Unit – The Gaithersburg Health Unit (HU) provides medical assistance and tracking of Occupational Health Records in addition to Personal Health Records. Each patient provides intake information that contains both Personally Identifying Information including Protected Health Information. Records from 2019 to present will**

be scanned into the EMRS, and all records going forward will be entered directly into the EMRS. Records prior to 2018 are stored in hard copy only and only within the HU's locked storage cabinets. There are two managed desktop Windows machines attached to spirometer and audiometer medical equipment that collect patient test results. The results from the diagnostic equipment are sent to the EMRS via HTTPS.

There are two Access databases that maintain records, including test results and date of birth of individuals who participate in certain medical programs and are used to track when tests are required. These databases are stored on an encrypted shared drive maintained by OISM (SSP 184-12). These databases have been replaced by the EMRS, but are retained for historical data. The historical data in these databases was not imported into the EMRS because the benefit was not worth the level of effort required to do so.

*g. Identify individuals who have access to information on the system*

RMS feeds are only made available to Emergency Service Divisions employees. In the event of an incident the recordings may be made available to law enforcement entities.

Only radiation physicists within NIST who have a need to keep track of radioactive material have access to HAPPY. In support of licensing, NIST is required to share information in HAPPY with the Nuclear Regulatory Commission (NRC) annually.

There is one NIST superuser with access to the ERMS configuration. There are 3 Health Care Providers who can write prescriptions, access patient data, and schedule appointments. There are 2 Health Unit Staff that perform administrative tasks. All NIST staff and associates with user accounts will have access to their own personal health information. Supervisors can also see if employees are in compliance with occupational health HU visits.

*h. How information in the system is retrieved by the user*

The RMS is a live camera feed of radioactive material viewed by NIST Emergency Services on a continuous basis. In the event of an incident, the recorded feed and the timestamp are used for retrieval by NIST Emergency Services staff. Otherwise, the recorded feed is not retrievable by the end user.

HAPPY data is retrieved by authorized individuals by opening the database and retrieving the source by type of radioactive source. Radioactive source owners can retrieve their data by their name. SET information is available for retrieval by the end user. Otherwise, the HAPPY data is not retrievable by the end user.

The Health Unit paper case files are retrieved from secure file cabinets by authorized health practitioners or health unit administrative staff, by patient name. The online EMRS records are accessible by health practitioners, health unit administrative staff, and system administrators, and limited based on their role. They are retrieved by patient name or by employee ID. Online EMRS records are accessible by the end user through single sign-on (SSO).

**Tort records are stored and retrieved by name and date of incident.**

*i. How information is transmitted to and from the system*

**The RMS is viewed by NIST Emergency Services over an encrypted isolated REN network via TCP/IP. The information is not transferred to another system on a routine basis. In the event of an incident, the recording may be required for investigative and prosecuting purposes and would be shared through secure means.**

**The HAPPY does not automatically transmit information to other systems. Annually, a mandatory report is generated to provide the Nuclear Regulatory Commission and is sent via encrypted secure file transfer to ensure the report is only available to NRC.**

**The EMRS information is stored in Health Unit databases and encrypted in transit to the EMRS interface via HTTPS. Paper-based medical case files are not electronically transmitted. Patients can request paper copies which are then given directly to them.**

**Paper records associated with Torts or workers' compensation are exchanged either in envelopes marked, "For XXXX's Eyes Only" or hand delivered to the recipient. To request information from the Emergency Services Office, an OSHE employee fills in a NIST-1226 with justification for requesting ESO physical security related information. The Police Chief reviews the police report to ensure it does not contain any law enforcement sensitive information, and then forwards to OSHE via an encrypted email. The report typically includes the names of personnel involved, contact information, and a synopsis of what occurred. Electronic records are exchanged via encrypted email or secure files shares such as Kiteworks or nfiles. The NIST claims specialist who handles Tort claims and the Incident Investigation Specialist handling compensation claims have been trained on handling PII in electronic and paper format and provides detailed instructions on how to submit data to individuals involved. Information is gathered by OSHE for investigation purposes only. Information for Tort claims are sent to legal and/or finance and the claimant for retention. Working copies are destroyed or deleted. For OSHA recordables and Workers Compensation, investigative information is put into DOC and OSHA systems and PII is not retained by OSHE.**

## **Questionnaire:**

1. The status of this information system:

**This is an existing information system with changes that create new privacy risks.**

*Complete chart below, continue to answer questions, and complete certification.*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>
<b>Significant System Management Changes</b>
Other changes that create new privacy risks:

--

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

**Yes**

<b>Activities</b>
<b>Video surveillance</b>
<b>Other</b>
Other activities which may raise privacy concerns:
<b>Collection of sensitive PII</b>

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

**No, this IT system does not collect any BII.**

4. Personally Identifiable Information (PII)

- 4a. Does the IT system collect, maintain, or disseminate sensitive personally identifiable information (PII)?

As per OMB 17-12: “The term PII refers to information that can be used to distinguish or trace an individual’s identity either alone or when combined with other information that is linked or linkable to a specific individual.”

**Yes**

The IT system collects, maintains, or disseminates sensitive PII about:

**DOC employees**

**National Institute of Standards and Technology Associates**

**Contractors working on behalf of DOC**

**Other Federal Government personnel**

**Members of the public**

*If the answer is “yes” to question 4a, please respond to the following questions.*

- 4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?



**Yes**

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
<b>The collection of SSN is required for reporting to the Nuclear Regulatory Commission and is collected in HAPPY.</b>
<b>The paper copies of the Health Unit Occupational Health records will continue to collect the SSN in order to archive to NARA. When the EMRS is in use, the SSN will not be stored. Upon archival, a report will be run to generate a cover page for the medical record, printed, placed in the archival envelope, and sent to NARA.</b>
Provide the legal authority which permits the collection of SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

**Yes, the IT system collects, maintains, or disseminates PII other than user ID.**

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

**No, the context of use will not cause the assignment of a higher PII confidentiality impact level.**

*If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.*

Is a PIA Required?	<b>Yes</b>
--------------------	------------

## CERTIFICATION

  X   I certify the criteria implied by one or more of the questions above **apply** to the 150-01 Office of Safety, Health, and Environment and as a consequence of this applicability, I will perform and document a PIA for this IT system.

       I certify the criteria implied by the questions above **do not apply** to the 150-01 Office of Safety, Health, and Environment and as a consequence of this non-applicability, a PIA for this IT system is not necessary.


Name of System Owner (SO):

Banovic, Stephen     **STEPHEN BANOVIC**     Digitally signed by STEPHEN BANOVIC  
 Signature of SO: \_\_\_\_\_ Date: 2022.01.27 12:31:24 -05'00'     Date: \_\_\_\_\_

Name of Co-Authorizing Official (Co-AO):

Mackey, Elizabeth     **Mackey, Elizabeth A.**     Digitally signed by Mackey, Elizabeth A. Dr. (Fed)  
 Signature of Co-AO: **Dr. (Fed)**     Date: 2022.01.28 15:50:33 -05'00'     Date: \_\_\_\_\_

Name of Chief Information Security Officer (CISO):

Heiserman, Blair          Digitally signed by BLAIR HEISERMAN  
 Signature of CISO: \_\_\_\_\_ Date: 2022.01.28 10:49:17 -05'00'     Date: \_\_\_\_\_

Name of Authorizing Official (AO):

Sastry, Chandan     **CHANDAN SASTRY**     Digitally signed by CHANDAN SASTRY  
 Signature of AO: \_\_\_\_\_ Date: 2022.01.27 12:32:54 -05'00'     Date: \_\_\_\_\_

Name of Privacy Act Officer (PAO):

Fletcher, Catherine     **CATHERINE FLETCHER**     Digitally signed by CATHERINE FLETCHER  
 Signature of PAO: \_\_\_\_\_ Date: 2022.01.27 13:51:06 -05'00'     Date: \_\_\_\_\_

Name of Chief Privacy Officer (CPO):

Barrett, Claire     **CLAIRE BARRETT**     Digitally signed by CLAIRE BARRETT  
 Signature of CPO: \_\_\_\_\_ Date: 2022.01.27 11:03:24 -05'00'     Date: \_\_\_\_\_